TEXNİKA ELMLƏRİ

TECHNICAL SCIENCES

DOI: https://doi.org/10.36719/2663-4619/97/159-163

Sərdar Qasımov
Azərbaycan Dövlət Neft və Sənaye Universiteti
fizika-riyaziyyat elmləri üzrə fəlsəfə doktoru
sardarkasumov1955@mail.ru
Səbinə Dadaşzadə
Bakı, Azərbaycan
sabinaxva9818@gmail.com

RESURS MƏHDUDİYYƏTLİ İNTERNET PLATFORMALARI ÜÇÜN ADAPTİV TƏHLÜKƏSİZLİK ÇƏRÇİVƏSİ

Xülasə

İşin əsas məqsədi adətən resursları məhdud cihazlardan ibarət olan, xüsusilə Simsiz Sensor Şəbəkələri (WSN) üçün uyğun olan, dinamik olaraq tənzimlənən təhlükəsizlik metodunu araşdırmaq və müəyyən etməkdir.

Həm yüksək səviyyəli təhlükəsizlik, həm də batareya ilə işləyən simsiz cihazların uzun ömür ehtiyacını dəstəkləmək və təhlükəsizlik giriş vaxtının səviyyəsini tənzimləmək üçün çevik vasitələrə ehtiyac var. Bu məqsədlə, məqalədə simsiz sensorlar və şlüz arasında təhlükəsizliyin əsas komponenti kontekstdən asılı olaraq tələb olunan təhlükəsizlik səviyyəsini seçə və resursa bu barədə məlumat verə bilən Adaptiv Təhlükəsizlik Meneceri (ASM) olan bir həll təklif edilir. Bu, lazım olduqda həm yüksək səviyyəli təhlükəsizlik, həm də batareya ilə işləyən simsiz cihazların uzun ömür müddətini dəstəkləməyə imkan verir. ASM-dən gələn əmrlərə əsasən, simsiz sensorlar əvvəlcədən paylaşılan açarlardan (PSK) uyğun açarı seçə bilər.

Açar sözlər: *Adaptiv Təhlükəsizlik, əşyaların interneti, simsiz sensorlar şəbəkəsi, məhdud cihaz, Adaptiv Təhlükəsizlik Meneceri (ASM)*

Sardar Gasimov
Azerbaijan State Oil and Industry University
PhD in physical and mathematical sciences
sardarkasumov1955@mail.ru
Sabina Dadashzadeh
Baku, Azerbaijan
sabinakhva9818@gmail.com

An adaptive security framework for resource-constrained internet platforms

Abstract

The aim of this work is to investigate and define adynamically adjustable security method, suitable especially for Wireless Sensor Network (WSNs), usually composed by resource constrained devices. In order to support both the high level of security and the need for long lifetime of battery powered wireless devices, flexible means to adjust the level of security at run time is needed. To this end, the paper proposes a solution, whose main component in the security between wireless sensors and the gateway is an Adaptive Security Manager (ASM), which select the required level of security and inform the resource about it, based on the context. This makes it possible to support both high level of security and long lifetime of battery powered wireless devices when needed.

Based on commands from the ASM, wireless sensors can select the suitable key from pre-sharedkeys (PSKs).

Keywords: *Adaptive Security, internet of things, wireless sensors network, constrained device, Adaptive Security Manager (ASM)*

Giriş

Məqalə uyğunlaşdırılmış təhlükəsizliklə bağlı əməliyyatların həyata keçirilməsində həyata keçirilən həllin nə dərəcədə effektiv olduğu barədə təfərrüatları təqdim etmək məqsədi daşıyır. Məqalədə bir ASM instansiyasının bütün şəbəkə yeniləmə prosedurunu həyata keçirməyə cavabdeh olduğu və hər bir xidmət istehlakçısının digərlərinin eyni şəbəkə interfeysində qeydiyyata alındığı zaman baş verən performansları təsvir edir. Paralelliyin maksimum səviyyəsi sistem əməliyyatlarını yerinə yetirmək üçün tələb olunan iş yükü şəbəkə interfeysləri arasında bərabər bölüşdürüldükdə əldə edilir. Əksinə, əməliyyatlar yalnız bir interfeysə aid olduqda, paralellik yalnız iki səviyyəyə endirilir, çünki dispetçerin operativliyinə töhfə verən hər bir ip, əməliyyatı başa çatdırmaq üçün interfeysi kilidləməlidir, buna görə də digər iplər öz növbələrini gözləmək məcburiyyətində qalırlar.

Hazırda informasiya təhlükəsizliyi və informasiya texnologiyaları sahəsində insidentlərin (cinayətlərin) sayında artım müşahidə olunur. Buna şəbəkə saxlama texnologiyalarının geniş yayılması və IoT əşyalarının geniş tətbiqi kömək edir: 2018-ci ildə qoşulmuş cihazların sayı 22 milyard qiymətləndirilirdi və 2025-ci ilə qədər təxminən 40 milyarda çatacaq (Strategy Analytics tədqiqat şirkətinin məlumatları). Bu cihazlarda kibercinayətkarlar tərəfindən istifadə edilə bilən zəifliklər ola bilər və nəticədə istifadəçi məxfiliyinə və ictimai təhlükəsizliyinə xələl gətirir (Habtamu, Dattani, 2008: 191-196). Beləliklə, təhlükəsizlik IoT ilə əlaqəli əsas problemlərdən biridir. Bu problemin səbəbi, əksər istehlakçı texnologiyaları kimi, IoT texnologiyalarının təhlükəsizlik nəzərə alınmaqla dizayn edilməməsidir, çünki istehsalçıların əsas məqsədi maya dəyərini və inkişaf vaxtını minimuma endirmək, istehsalın maya dəyərini azaltmaq və istehsal həcmini artırmaq idi. Bu siyasət nəticəsində ağıllı cihazlar resurslardan məhrumdur. Bu çatışmazlığa görə, əksər təhlükəsizlik alətləri IoT cihazlarında quraşdırıla bilmir, bu da cihazları kibercinayətkarlıq üçün asan hədəfə çevirir. Hakerlər daxili təhlükəsizlik sistemlərində zəif cəhətləri, onların zəifliklərini tapır və IoT cihazlarından digər saytlara hücum etmək üçün alət kimi istifadə edə bilərlər (Habtamu, Dattani, 2008: 191-196). IoT texnologiyaları ilə silahlanmış kibercinayətkarlar virtual məkanda olarkən insanların təhlükəsizliyini və hətta həyatını təhdid edə bilər və belə cinayətlərin sayı getdikcə artır. Bu kimi təhlükələr mühüm sual doğurur: ağıllı cihaz istifadəçiləri özlərini necə qoruya bilər? Təhlükəsizlik mütəxəssisləri parolların dəyişdirilməsini, tətbiqlərin və cihazların özünü yeniləməyi və şəxsi məlumatların qorunmasını tövsiyə edir (Wahab, Bentahar, Otrok, Azzam, 2016: 123).

Çox vaxt IoT-də məhdud resurs cihazları 16 kB-dan az RAM və 128 kB yaddaş sahəsinə malikdir, məsələn, açar uzunluqlarını məhdudlaşdırır. Resurs məhdudiyyətlərinə əlavə olaraq, rabitə də səhvlərə meylli ola bilər. IoT cihazlarının uzaqdan və paylanmış işləməsi cihazlara fiziki hücum etməyi də mümkün edir. Beləliklə, təcavüzkarlar fiziki hücum edərək cihazlardan təhlükəsizlik açarı əldə edə bilərlər. Resurs məhdudiyyətləri tez-tez cihazları tam müdaxiləyə qarşı məhdudlaşdırır (Arbor Networks, 2010).

Tələb olunan təhlükəsizlik səviyyəsi ötürüləcək məlumatların xarakterindən asılıdır, lakin lazımi təhlükəsizlik səviyyəsinə cihazların yeri də təsir göstərə bilər. Hücumlar üçün daha yüksək risk varsa, tələb olunan təhlükəsizlik səviyyəsi də daha yüksək olur. Buna görə də, təhlükəsizlik mexanizmləri dəyişikliklər üçün çevik olmalıdır. Bu korrelyasiya WSN - lərdə statik təhlükəsizlik həllərinin tətbiq oluna biləcəyini yenidən nəzərdən keçirməyə və təhlükəsizlik səviyyəsinin daha sabit olmadığı, lakin şəbəkə statusuna uyğun olaraq dinamik olaraq təyin olunduğu adaptiv model haqqında daha çox düşünməyə səbəb olur (Anthes, 2010: 67).

This section presents and analyzes a set of solutions about.

Adaptiv Təhlükəsizlik Çərçivəsi şəbəkə təhdidləri, mövcud enerji və hər bir qovşağın yaddaşı kimi WSN statusu məlumatlarına əsaslanır. Çərçivə TinyOS-da tətbiq edilib və üç moduldan

ibarətdir: *Kontekst modulu* - O, ayrılmış modullarla təmsil olunmaqla tələb olunan aspektlərin hər birində cari şəbəkə vəziyyətini təmsil edir. *Təhlükəsizlik Uyğunlaşması* - Şifrələmə və istifadə ediləcək autentifikasiya alqoritmləri baxımından şəbəkə üçün adekvat təhlükəsizlik səviyyəsini müəyyən etmək üçün kontekst modulu tərəfindən yaradılmış məlumatlara əsaslanır. *Təhlükəsizlik səviyyəsi* - Hər biri xüsusi təhlükəsizlik səviyyəsinə uyğun gələn və hər biri yuxarıda qeyd olunan autentifikasiya və şifrələmə alqoritmlərinin birləşməsi kimi müəyyən edilmişdir. Bu həll bütün tələb olunan açarları yerləşdirmək üçün kifayət qədər yaddaş sahəsi tələb edir (Chang, 2012).

Genetic Message Oriented Middleware (GEMOM) şəbəkə qurumları arasında şəbəkə resurslarının mesaj mübadiləsini dəstəkləməyə həsr olunmuş çərçivədir. O, artıq şəbəkə qovşaqlarını yaxşı miqyaslaya bilir (Chang, 2012). Sistem məlumat mübadiləsi üçün dərc/abunə paradiqmasına əsaslanır. Çərçivə təhlükəsizlik, xidmət keyfiyyəti, autentifikasiya, avtorizasiya və anomaliyaların aşkarlanması kimi şəbəkə aspektləri üzərində monitorinq əməliyyatlarını həyata keçirmək üçün ayrılmış bir neçə modula əsaslanır. Şəbəkə boyu toplanmış məlumatlardan qiymətli nəticələr çıxarmaq üçün bir neçə təhlükəsizlik göstəriciləri müəyyən edilmişdir (Chang, 2012). Şəbəkənin arzuolunmaz vəziyyətdə olduğu hesab edilərsə, sistem düzəldici əməliyyatlar həyata keçirməyə cəhd edir.

Şəbəkəyə bağlı DC motor sistemi üçün birgə təkamüllü genetik alqoritm (CGA) üzrə istifadə halı kimi qəbul edilmişdir. CGA alqoritmini sınamaq üçün Simulink - ə əsaslanan test tətbiq edilmişdir, onun effektiv şəkildə paylanmış kiberfiziki sistemin təhlükəsizlik - performans mübadilə modeli üçün optimal həlləri qaytardığını nümayiş etdirən nəticələr əldə edilmişdir.

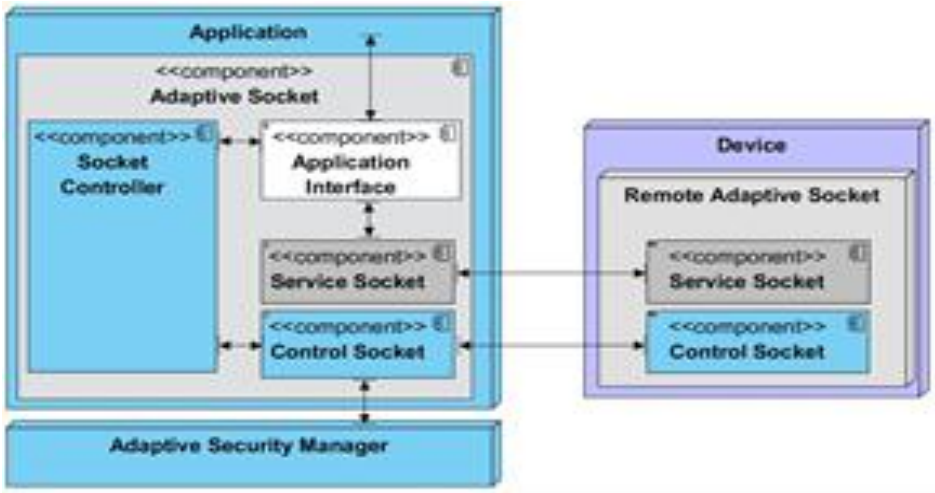
Uyğunlaşma anlayışı ənənəvi təhlükəsiz bağlantılar haqqında bəzi mülahizələrdən başlayaraq formalaşdırıla bilər. Onlar iki son nöqtə arasında qorunan əlaqəni dəstəkləyən avtonom və özünü idarə edən qurumlardır. Təhlükəsizlik protokolu xarici müdaxiləyə ehtiyac olmadan rabitə zamanı onları idarə etməkdən məsuldur. Bu keçidlərdə adaptiv təhlükəsizliyi təmin etmək üçün şəbəkənin təhlükələrə məruz qalma səviyyəsi nəzərəçarpacaq dərəcədə dəyişdikdə təhlükəsizlik parametrlərinin yayımına cavabdeh olan idarəetmə bölməsi ilə əlavə aktiv əlaqə saxlamaq tələb olunur. Yeni parametrlər, çox ehtimal ki, tətbiqin əməliyyatlarına nəzərəçarpacaq dərəcədə təsir etmədən artıq qurulmuş təhlükəsiz bağlantılara tətbiq edilməlidir (Savola, Heinonen, 2010: 25-34).

Arxitekturanın əsas komponentlərindən biri həm ənənəvi socketin xidmət xüsusiyyətlərini, həm də ASM - dən təlimat almaq və onları tətbiq etmək üçün lazım olan idarəetmə xüsusiyyətlərini özündə birləşdirən Adaptiv Soketdə (AS) sarğı sinifidir. Bu komponent proqramın məlumat mübadiləsi üçün istifadə etdiyi xidmət yuvasına möhkəm bağlanmalıdır.

ASM, nüvə səviyyəsində işləyən təhlükəsizlik protokollarına nəzarət etmək üçün nüvə ilə əlaqə kanalı yaratmaq üçün tələb olunan inzibati imtiyazlarla yaradılmalı olan müasir bir maşında işləyən bir demon prosesidir. ASM, Şəbəkə Təhlükəsizliyi Qiymətləndiricisinin (NSE) təhlükəsizlik səviyyəsinin yeniləmə sorğusu verməsini gözləməyə cavabdehdir. Həqiqətən, NSE şəbəkə təhlükəsizliyi təhlilini həyata keçirir və tələb olunan təhlükəsizlik səviyyəsi haqqında məlumat verir. Şəbəkə təhlili bu məqalənin əhatə dairəsinə daxil deyil və ədəbiyyatda mövcud olan istənilən yanaşmadan istifadə etməklə həyata keçirilə bilər (Arora, 2012: 90).

ASM sorğuları emal edir və onun etibarlılığını qiymətləndirir. Sorğu daha sonra adaptiv təhlükəsizlik xidmətinə, yəni uzaq ASM - lərə və adaptiv rozetkalara töhfə verən bütün digər sistem komponentlərinə yayımlanır. Nəzarət blokunun müdaxiləsinin son nöqtələrin autentifikasiyası və təhlükəsiz kanal üçün seans konfiqurasiyasının təmin edilməsi ilə məhdudlaşdığı mərkəzləşdirilmiş həllərə baxmayaraq, burada ASM - in rolu daha çoxdur; həqiqətən də, onun müdaxiləsi hər bir şəbəkə təhlükəsizlik səviyyəsi dəyişikliyində tələb olunur (Habtamu, Dattani, 2008: 191-196).

Şəkil 1 cihaz və proqram səviyyəsində AS-nin arxitekturasını və onun ASM ilə əlaqəsini göstərir. Xüsusilə, Tətbiq İnterfeysi quraşdırılmış xidmətə girişi təmin edir və proqram ilə xidmət arasında qarşılıqlı əlaqəyə vasitəçilik edir, Socket Controller isə AS-ni idarə edən məntiqi təmsil edir. Socket Controller ASM və ya uzaqdan AS tərəfindən göndərilən əmrləri emal edir. Təhlükəsiz kanal parametrlərini yeniləmək üçün sorğu olduqda, o, Tətbiq İnterfeysindən istifadə edir və xidmət yuvasına doğru bütün əməliyyatları dayandırır (Department of the Army, 2010: 3).



Şəkil 1. Adaptiv Soket arxitekturası

Arxitektura sistemə simsiz sensorlar və ya mobil telefonlar kimi resursları məhdud olan cihazlara xidmət göstərməyə imkan verir. Bu cihazlarda yaradılmış AS - lər sadəcə olaraq bir ASM - də uzaq istehlakçılar kimi qeydiyyatdan keçə bilər. Birdən çox ASM nümunələri yaradıla və əməkdaşlıq edən qrup yaratmaq üçün konfiqurasiya edilə bilər (Chow, Chow, 2012: 301).

ASM-lərin hər bir qrupunda uyğunlaşma xidmətinin koordinatoru kimi çıxış edən əsas nümunə olmalıdır, qalan nümunələr isə verilən direktivləri yerinə yetirmək üçün məhduddur. Şəbəkədə yerləşdirilmiş hər bir ASM adaptiv təhlükəsizlik xidmətinə, onun üzərində qeydə alınmış socketə çıxışı təmin edir. Bundan əlavə, müvafiq ASM-lər vasitəsilə qarşılıqlı olaraq əlçatan olmaq üçün eyni ASM-lər qrupunda iki adaptiv socketin qeydiyyata alınması tələb olunur. AS-lər ASM - i işlədən eyni maşında yaradıla bilər. Bu halda autentifikasiya və qeydiyyat yerli host rabitəsindən istifadə etməklə həyata keçirilir.

Həll bir neçə paylanmış nümunəyə əsaslandığı üçün etibarlı vaxt sinxronizasiya protokolu qəbul edilməlidir. Bu protokol baxılan sənədin əhatə dairəsindən kənardadır, çünki o, həllin tətbiq olunduğu hər bir WSN üçün xarakterikdir (Gheorghe, Rughinis, 2012: 636-641).

ASM nümunələrinin yerləşdirilməsi mövcud şəbəkə arxitekturasının forması ilə bağlı heç bir xüsusi fərziyyə irəli sürmür. Həqiqətən, o, məntiqi olaraq ayrılmış çoxlu şəbəkələri əhatə edə bilən, lakin yenə də eyni şəbəkə qatı protokolundan istifadə edən abstraksiya səviyyəsində işləyir. ASM müxtəlif İP versiyaları ilə işləyən iki şəbəkənin ayrılması zamanı yerləşdirilmiş sərhəd qovşağında da yerləşdirilə bilər. Bununla belə, istifadəçinin fərqli bir IP versiyası ilə işləyən şəbəkədə yerləşdirilmiş resursa çata bilməsi üçün relay imkanları olan vasitəçi proqram tələb olunur. Bu proqram ASM sərhədində qeydiyyata alınmalı və iki adaptiv socket yaratmalıdır. Tətbiqin vəzifələri bir socketdən gələn paketləri məzmununu dəyişdirmədən digərinə yönləndirməkdən ibarətdir. Bu həll, uzaq təşkilatın WSN - də yerləşdirilmiş resurslara daxil olmaq niyyətində olduğu simsiz sensor şəbəkələrində olduqca genişdir (Arora, 2012).

Həm ASM, həm də AS-lər (və onlar arasındakı əlaqə) təhlükəsizlik səviyyəsinin yersiz aşağı düşməsinə səbəb ola biləcək zərərli hücumlardan autentifikasiya və şifrələmə üsullarından istifadə etməklə qorunur. Məkan səbəblərinə görə, bu məqalədə həllin tam təhlükəsizlik təhlili aparıla bilməz (Chow, Chow, 2013: 394).

Sistemin inkişafı prosesi SatisFatory layihəsindən irəli gələn tələblərə uyğun olaraq qurulmuşdur. Layihə C++ kitabxanalarının intensiv istifadəsi ilə C++ dilindən istifadə etməklə hazırlanmışdır: STL (abstraksiya və daşınma qabiliyyəti), Boost (platformalar arası yuvalar) və OpenSSL (təhlükəsizlik). MySQL DBMS3 funksiyaları xüsusi olaraq müəyyən edilmiş cədvəllər daxilində istifadəçilər, resurslar, ASM-lər, parametrlər və təhlükəsiz keçidlərin açarları haqqında məlumatı saxlamaq və bərpa etmək üçün istifadə edilmişdir (Arora, 2011: 23).

Nəticə

Məqalədə şərh olunan yanaşmalar adaptiv təhlükəsizlik vasitəsilə gücü artırmaq üçün necə istifadə oluna biləcəyini göstərir.

Təklif olunan çərçivə sonralar tək adaptiv təhlükəsizlik təminatından kənara çıxan məlumat mübadiləsi üçün protokoldan istifadə etməlidir.

Bundan əlavə, sistemlər resursların statusunu nəzərə alaraq (yəni enerjinin mövcudluğu azdırsa, onu təhlükəsiz əlaqələrin yaradılmasını dəstəkləməlidir.

Ədəbiyyat

1. Habtamu, A., I., Dattani, M., Novkovic, J., Bigham, S., Topham, Savola, R. (2008). Gemom - significant and measurable progress beyond the stateof the art. In Systems and Networks Communications. ICSNC ’08.3rd International Conference on, pp.191-196.
2. Wahab, O.A., Bentahar, J., Otrok, H., Azzam, M. (2016). How to distribute the detection load among virtual machines to maximizethe detection of distributed attacks in the cloud? IEEE International Conference on Services Computing, 123 p.
3. Arbor Networks. (2010). Worldwide Infrastructure Security Report.
4. Anthes, G. (2010). “Security in the Cloud.” Communications of the ACM, November, 67 p.
5. Chang, R. (2012). “Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial”. IEEE Communications Magazine, October.
6. Savola, R.M., Heinonen, P. (2010). Security-measurability-enhancing mecha-nisms for a distributed adaptive security monitoring system. In Emerging Security Information Systems and Technologies (SECURWARE). Fourth International Conference on, pp.25-34.
7. Department of the Army. (2010). Physical Security. Field Manual FM, pp.3-99.
8. Chow, W.Z., Chow, M.Y. (2012). Optimal Trade off Between Performance and Security in Networked Control Systems Based on Coevolutionary Algorithms, IEEE Transactions on Industrial Electronics, 301 p.
9. Gheorghe, L., Rughinis, R., Tapus, N. (2012). Adaptive Security Framework for Wireless Sensor Networks, Fourth IEEE International Conference on Intelligent Networking and Collaborative Systems, pp.636-641.
10. Arora, M. (2012). “How Secure Is AES Against Brute-Force Attack?” EE Times, May 7, 90 p.
11. Arora, K. (2011). “Impact Analysis of Recent DDoS Attacks”. International Journal on Computer Science and Engineering, Vol. 3, № 2. February, 23 p.
12. Chow, W.Z., Chow, M.Y. (2013). Modeling and Optimizing the Performance-security Trade-off in D-NCS Using the Coevolution-ary Paradigm, IEEE Transactions on Industrial Information, pp.394-402.

Göndərilib: 02.10.2023 Qəbul edilib: 28.11.2023